WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

PCT **WIPO**

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) IPC[6]:		(11) International Publication Number: WO 99/23614
G07C 9/00, B60R 25/00	A1	(43) International Publication Date: May 14, 1999 (05/14/99)

(21) Int. App. No.: PCT/DE98/03182

(22) Int. App. Date: October 30, 1998 (10/30/98)

(30) Priority Data:
197 48 325.9 October 31, 1997 (10/31/97) DE

(71) Applicant: *(for all designated States except US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D-80333 Munich (DE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: LÖFFLER, Maximilian [DE/DE]; Wanderweg 8a, D- 93170 Bernhardswald (DE).

(74) Common agent: SIEMENS AKTIENGESELLSCHAFT; P.O. Box 22 16 34, D-80506 Munich (DE).

(81) Designated states: BR, CN, JP, KR, MX, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
With international search report.
Before the expiration of time limit for amending the claims; to be republished in the event of receipt of amendments.

(54) Title: SECURITY DEVICE AGAINST UNAUTHORIZED USE, ESPECIALLY OF A MOTOR VEHICLE

(57) Abstract

The security device comprises a receiver (2) that receives comparative data from control center (6) via a communications system. The comparative data are stored in a setpoint storage (11). In order to gain access to the object (1), biometric characteristics of a user are detected and compared with the stored comparative data. Use of the object (1) is enabled in the event of a match.

Description

Security device against unauthorized use, especially of a motor vehicle

The invention relates to a security device against unauthorized use, in particular of a motor vehicle, such as a lease or rental vehicle or a fleet vehicle. With this security device, use of an object, in particular the use of a motor vehicle should be possible only upon proof of authorization.

In a known security device (DE 195 08 370 Al), bidirectional communication takes place between a motor vehicle and a control center. Release signals are transmitted by the control center to the motor vehicle. With the release signal, a use restriction of the vehicle is also specified. When a user opens his vehicle with a key, a query is made as to whether there is an authorization for use. If there is an authorization, the vehicle can be used to the extent communicated with the release signal.

When an unauthorized individual comes into possession of the key, he can use the vehicle as long as the release signal transmitted by the control center is present. If it is not yet known in the control center that the vehicle has been stolen, the unauthorized individual can continue to use the vehicle.

Another known security device (US 4,353,056 or DE 42 22 387 C2) has a biometric identification arrangement with which a fingerprint of a user is detected before access to the vehicle is released. With such security devices, only the initially specified user can use the vehicle to a defined extent. If a lease or rental vehicle changes owner or user, the authorization data of the new user must be stored in advance in the vehicle so that he can properly use the vehicle.

The object of the invention is to reliably and simply prevent unauthorized use of an object, in particular of a lease or rental vehicle or a fleet vehicle.

This object is accomplished according to the invention through the characteristics of claims 1 and 8. The security device has, on the one hand, a biometric identification arrangement with which biometric characteristics of a user are detected. Upon access to the motor vehicle, these biometric characteristics are compared with stored comparative data. In the event of a match, the use of the vehicle is permitted. In order that the comparative data can be changed at any time, the security device has, on the other hand, a receiver, by which the authorization data are received via a communications system. These authorization data are stored either as comparative data or used to introduce initialization and subsequent storage of the comparative data.

With this security device, the lease or rental vehicle can be passed on to a different owner, with the authorization data previously acquired in a control center and transmitted by the communications system to the vehicle. Not all authorization data of each future user has to be stored in the vehicle. Users of a vehicle may, consequently, change at will as long as they are recognized as users in the control center. Keys for use of the vehicle

need not be passed from one user to the next. It is possible for the data of only one user to be stored in the vehicle.

With a fleet of vehicles, it can thus be specified that a vehicle is used by a first driver and, after a specified time, by a second driver. The extent of the use can, in each case, be transmitted to the vehicle with the authorization data before the driver change.

With this security device, the initialization can occur at the location of the vehicle. However, the start of the initialization is released by the control center.

Advantageous embodiments of the invention are characterized in the dependent claims. Thus, the biometric identification arrangement can be a fingerprint recognition unit, a voice recognition unit, or an image recognition unit with which the biometric characteristics of a user are detected. A user thus need not carry a key with which he must unlock the vehicle and can start the vehicle.

If the biometric characteristics detected match the comparative data, both a central locking system and a drive-off lock can be controlled. The biometric identification arrangement is preferably arranged on or in the vehicle such that a biometric identification can be performed both with users who come from the outside and are seated in the vehicle. Preferably, the identification arrangement is disposed on or in the vicinity of a lock (door lock or ignition lock) of a vehicle. Thus, both the access to the vehicle and the starting of the vehicle are permitted only with authorization.

The authorization data can be person-specific biometric data or even object-specific use data with which the extent of the use is specified. Control data can also be transmitted as authorization data, based on which an initialization is started, and upon successful completion of which, comparative data of the user performing the initialization are stored. The initialization is performed when a PIN number is correctly entered via a keyboard.

Exemplary embodiments of the invention are explained in detail in the following with reference to the schematic drawings. They depict:

Fig. 1:	a motor vehicle with a security device according to the invention that communicates via a communications system with a control center,
Fig. 2:	a schematic diagram of the security device according to Fig. 1,
Fig. 4 [sic]:	a schematic diagram of the biometric identification arrangement,
Fig. 3 [sic]:	a biometric identification arrangement that is disposed on a door handle, and
Fig. 5:	another exemplary embodiment of the biometric identification arrangement.

A security device against unauthorized use of an object according to the invention is explained in the following using the exemplary embodiment of the use of a motor

vehicle. The security device can also be used with many other objects with which authorization must be proved before the use of the object.

A vehicle 1 (Fig. 1) has a transmitting and receiving device 2 (cf. also Fig. 2) that is connected with an antenna 3 in or on the vehicle 1. The transmitting and receiving device 2 is connected with a control unit 4, in which received data are evaluated and data to be transmitted are prepared. The control unit 4 is also connected with a biometric identification arrangement that detects biometric characteristics of a user and processes them into identification data. The transmitting and receiving device 2 in the control unit 4 are supplied with power by a motor vehicle battery 5.

The security device in the motor vehicle 1 communicates with a control center 6 via a communications system. The control center 6 can transmit data to the vehicle 1 via a transmitting/receiving antenna 7 and receive the like therefrom.

The communications system can be, for example, a mobile telephone or mobile radio system with which the vehicle's telephone system can automatically make a connection with the control center 6. The communications system can also be a satellite communications system with which data are transmitted by a control center 6 via geostationary satellites to the motor vehicle 1 and vice versa. The communications system can also be a special radio system with which a data transmission between an object and a control center 6 occurs. The design of the communications system is not essential to the invention. What is essential is that data are transmitted between a control center 6 and an object.

The data transmission between the vehicle 1 and the central office 6 or vice versa occurs in encrypted/encoded form; thus, overhearing the data and their use by unauthorized individuals is rendered difficult. The data always include an object- or vehicle-specific answerback code so a mixup of vehicles is prevented.

The security device on the vehicle side has the transmitting and receiving device 2 (Fig. 2) that receives signals from the control center 6 via the antenna 3. These signals are demodulated and converted in the transmitting and receiving device 2 and sent to the central control unit 4. Biometric data that are detected by the biometric identification arrangement at the time of desired access to the motor vehicle are also sent to the control unit 4.

A fingerprint recognition unit 8 is advantageously used as an identification arrangement. Likewise, an image recognition unit 9 or a voice recognition unit 10 can serve as an identification arrangement.

Accordingly, at the time of desired access, a fingerprint of a user is detected with the fingerprint recognition unit 8, a physical characteristic or biometric pattern, such as, for instance, the face of the user or the characteristic iris in the eye of the user with the image recognition unit 9, or the voice of the user with the voice recognition unit 10. The data

detected are converted (digitized) and fed prepared to the control unit 4. There, the data are evaluated.

The control unit 4 compares the identification data that were detected by the biometric identification arrangement with comparative data that are stored in setpoint storage 11. The comparative data are those data that are anticipated when a user is authenticated (proof of his authorization).

If at least a portion of the identification data detected matches the stored comparative data, a control signal is generated and sent to a security unit, such as a central locking system 12 or a drive-off lock 13. Thus, the doors of the vehicle can be unlocked or the drive-off lock released.

The biometric identification arrangement, for vehicles, is preferably designed as a fingerprint recognition unit 8. This has a sensor 15 (Fig. 3) to detect the fingerprint, which is arranged on the body of the vehicle readily accessibly to the user from outside the vehicle 1. For the detection of the fingerprint, the user places one or a plurality of fingers 16 on the sensor 15. Depending on the detection mode, the "outer" fingerprint (ridge and valley pattern) or the "inner" fingerprint (structure of the epidermis) can be detected.

A signal is sent by a transmission element 17, e.g., optically or acoustically, to the sensor 15 with its sensor surface/touch surface 18. From the sensor surface 18, the signals go partially into the finger 16 or are reflected by its surface to the sensor surface 18. The signals returned from the sensor 15 as a result of reflection are received by a receiver element 19 and forwarded to the fingerprint recognition unit 8. The digitized and evaluated pattern of the fingerprint is sent to the control unit 4 and -- similarly as described in DE 42 22 387 C2 -- is further processed there.

The detection of the fingerprint may also occur with capacitive electrodes -- as described in the patent US 4,353,056. There are many other possibilities for detecting and evaluating the fingerprint. Since fingerprint recognition units and their mode of operation are adequately known, they will not be dealt with in greater detail here.

In order to be sure that the fingerprint is from a living person, a vitality detection unit 20 may also be present. In the exemplary embodiment according to Fig. 3, a pulse detection unit that detects the pulse of the finger 16 is provided as a vitality detection unit 20. Only when a pulse is detected are the detected fingerprint patterns compared with anticipated data that are stored in the setpoint storage 11. With at least a broad match, the central locking system 12 or the drive-off lock 13 is controlled.

There are many other known possibilities for establishing the vitality of the user. Thus, skin impedance measurements, pulsoximetric or electrocardiographic measurement processes, or other comparable processes can be carried out, which, however, will not be dealt with in detail here.

The sensor 15 for detection of the fingerprint may even be affixed on a door handle 21 (Fig. 4). The sensor 15 is advantageously arranged, protected, on the inside of the door handle 21. When a user pulls the door handle 21, at least one finger 16 lies on the sensor 15.

To keep the sensor 15 from becoming too dirty, a gasket 22 against which the door handle 21 rests sealingly in the unused state may be provided.

To detect the biometric identification data, the voice recognition unit 10 may also be used instead of the fingerprint recognition unit 8. In this case, a microphone 23 (Fig. 5) is arranged in the vehicle 1 such that it can detect the words spoken by a user. The words or voice patterns are then converted in the voice recognition unit 10 and evaluated as well as being further processed in the control unit 4.

The control unit 4 compares the voice signals received with reference signals that are stored in the setpoint storage 11. If the user is recognized as authorized using the words spoken, the door lock of the vehicle 1 is unlocked by the control unit 4.

The central locking system 12 comprises a driver door lock 24, a passenger door lock 25, two back seat door locks 26, a trunk lock 27, and - if present -a gas cap lock 28. These locks may be locked or unlocked by the control unit 4 partially individually or all together if the user is recognized as authorized.

When the vehicle 1 is unlocked, the user can enter the vehicle 1 and start the engine. A biometric authentication (fingerprint recognition, voice recognition, or image recognition) may also be a prerequisite for starting the engine. Consequently, an additional sensor to detect the fingerprint, an additional microphone to detect the voice, or a video camera 29 for image recognition are arranged in the interior of the vehicle 1. At the time of the attempt to start the vehicle, the biometric identification arrangement is activated. Upon successful authentication (authorization is proven), the vehicle can be used properly, since only then is the drive-off lock 13 released.

In the prior art, anticipated biometric data of a user are stored in the setpoint storage 11. These data were detected at the time of an initialization of the security device. Upon initialization, the user is authorized for the first time for the use of a vehicle 1, by storage of his authorization data.

With the security device according to the invention, the biometric data may be detected once or a plurality of times in a control center 6. There, each user who may use the vehicle may have his biometric characteristics in the form of identification data detected. The biometric data can remain stored in the control center 6, inaccessible to third parties.

Via the control center 6, the corresponding authorization data are transmitted - as needed - to the vehicle 1, i.e., the biometric data of the user who may use the vehicle are transmitted as authorization data to the vehicle. There, the authorization data are stored in the setpoint storage 11. In the process, the former authorization data may be overwritten

or deleted. Authorization data of a plurality of users may also be stored there at the same time. Then, a plurality of users may use the vehicle 1.

A new user may also be subsequently approved for the vehicle by having his authorization data detected by a biometric identification arrangement in the control center 6. The identification data detected are then transmitted to the vehicle as authorization data and stored in the setpoint storage 11.

Together with the authorization data, use data by which the extent of use of the vehicle 1 is specified may also be transmitted. The extent of use may be a time period, a geographic use area, a maximum travel distance, a number of users, or encoded information. The use data are transmitted encrypted or encoded as digital values to the vehicle 1 modulated along with the authorization data.

As soon as the authorization data are received, they are demodulated and decoded as well as being stored in the setpoint storage 11. The vehicle 1 is then ready for operation for the respective user to the extent specified in the use data.

The authorized extent of use can be monitored by known devices, such as a clock, a kilometer counter, a GPS positioning system, and the like. If the extent is exceeded, the user and the control center 6 can be warned. With an additional overrun, the vehicle 1 can be stopped from the control center 6 and locked, i.e., the user authorization is revoked.

As authorization data, an initialization control signal may also be transmitted along with encoded reference information, e.g., a PIN number, to the vehicle 1. If the PIN number made known to the user in advance is correctly entered via a keyboard 30 on the vehicle, the doors are unlocked and a learning procedure (called initialization) for person-specific biometric data is started. During the initialization, the identification data, once detected, are stored as authorization data. A new initialization can be performed only after a new initialization control signal is received from the control center 6.

Instead of a PIN number, other encoded information can be transmitted to the vehicle. Then -- instead of the keyboard 30 -- a different input means is required, with which encoded information is entered by the user. Such an input means may, for example, be a hand transmitter or a chip card made available by the lessor or fleet operator. These deliver their encoded information to the vehicle, where it is compared with the reference data received. In the event of a match, the learning procedure is started -- as described above.

For this, the fingerprint recognition unit 8, on whose sensor 15 the respective user places his finger 16, is, for example, activated. The fingerprint detected is processed and converted into comparative data. The comparative data are then stored in the set point storage 11. Upon completion of the initialization, this user can use the vehicle within the framework of the use specified.

This has the advantage that the user does not have to have previously been in the control center 6 in order to deposit his authorization data. However, he can only perform the initialization when, on the one hand, the initialization control signal has been received and, on the other, when an additional authorization has been verified. The additional authorization can be verified by entering the encoded information if the information entered matches the previously received reference information.

Time limits within which the initialization must be performed may be set for the initialization process. If the initialization is not performed during the set time, all previous comparative data may again be valid or they can be deleted such that no one is authorized to use the vehicle 1 unless new authorization data are again transmitted by the control center 6 or a new initialization is performed.

The PIN number transmitted must, for the sake of security, be known only to the vehicle lessor and the vehicle lessee, i.e., the user, in order to prevent improper use.

Provision can be made that the stored comparative data are valid for only a predefined time. After that, their validity expires. This can be accomplished in that the storage content of the setpoint storage 11 is deleted along with the comparative data. Then, new comparative data must be supplied to the setpoint storage 11 before the vehicle can be properly used again.

The biometric identification arrangement can be arranged substantially in the control unit 4 from which the connections to the sensor 15, the microphone 23, or the video camera 29 are made. The control unit 4 can be installed in an impenetrable housing.

Only the sensor 15, the microphone 23, or the video camera 29 for detection of the biometric characteristics have to be arranged in appropriate locations outside the control unit such that the biometric characteristics of a user can be detected simply.

Thus, the sensor 15 of the fingerprint recognition unit 8 can be arranged on the vehicle door and an additional sensor, in the vicinity of the ignition lock 31, on the dashboard within reach of the user, on the center console, or on the shift lever. The video camera 29 can be behind a windowpane of the vehicle such that it detects both the exterior and the interior of the vehicle. The microphone 23 is likewise arranged such that it can detect voice signals from both inside and outside. A plurality of microphones or a plurality of video cameras may also be present.

It is not essential to the invention what biometric characteristics are detected. What is essential is that the biometric characteristics detected are compared with the comparative data. For this, the comparative data are either transmitted via the control center 6 to the vehicle 1 and stored there in the setpoint storage 11 or are stored in the setpoint storage 11 after successful initialization as a result of an initialization signal received.

The setpoint storage 11 can be an EEPROM or another suitable data memory, whose data cannot be read from the outside by unauthorized individuals. The control unit 4 may be

essentially a microprocessor or a functionally equivalent device that controls the security device. The authorization data are exchanged as digital signals between the control center 6 and the vehicle 1 wirelessly in a suitable manner, for example, as HF signals.

The control unit 4 may be connected to the central locking system 12, the drive-off lock 13, or another security unit that can be locked or unlocked only if the comparison of the detected biometric identification data and the comparative data was successful.

In the case of other objects, such as, for instance, a hotel system, the communications system can be an in-house data network with multiple data lines. The authorization data are transmitted via the control center 6 to the individual security devices (in the case of hotels, these are the door locks). Thus, access authorization to the rooms can be controlled centrally. The hotel guest need only leave his fingerprint at reception. After departure of the guest, the authorization data for the room can be deleted centrally or overwritten with new authorization data of another hotel guest. In addition, a limited period of use can be provided through the use data.

The term "use" means both access to an object and use of the object itself. With a vehicle 1, use means both the unlocking of the door locks and release of the drive-off lock 13.

Motor vehicles, hotel rooms, garage doors, personal computers or telephones networked with a control center 6, and the like can be envisioned as objects. The security device according to the invention is used, in particular, for lease or rental vehicles. Likewise, freight companies can better protect their vehicle fleet (a plurality of trucks) from unauthorized use with the security device. The drivers can be forced by the use period to comply with rest periods as a result of the use data. The control office 6 can also receive an alarm signal when the extent of use is exceeded and can then make contact with the user -- for example, by telephone.

The term "drive-off lock 13" means an electronic device that enables starting an internal combustion engine and driving only upon proof of authorization. The device can, for example, be arranged in the engine valve equipment. It releases the operations of the engine valve equipment upon proof of authorization. The device can also electromagnetically control a valve in the fuel line. Likewise possible is a controlled switch in the ignition system that permits ignition of the internal combustion engine only after proof of authorization. A plurality of electronic devices distributed throughout the vehicle may also serve as drive-off locks.

Claims

1. Security device against unauthorized use, in particular of a motor vehicle (1), with
- a biometric identification arrangement (8, 9, 10) that detects biometric characteristics of a user and processes them into identification data,
- a receiving device (2) that receives authorization data via a communications system,
- a storage device (11) in which the authorization data received are stored as comparative data, and
- a control unit (3) [sic] that compares at least a portion of the identification data with the stored comparative data and controls a security unit (12, 13) depending on the result of the comparison.

2. Security device according to claim 1, characterized in that [the] identification arrangement is a fingerprint recognition unit (8).

3. Security device according to one [sic] claim 1, characterized in that the identification arrangement is a voice recognition unit (10).

4. Security device according to claim 1, characterized in that the identification arrangement is an image recognition unit (9).

5. Security device according to one of the preceding claims, characterized in that the security unit is implemented through a central locking system (12) and/or a drive-off lock (13).

6. Security device according to one of the preceding claims, characterized in that at least a portion of the identification arrangement (8, 9, 10) is arranged accessibly outside the vehicle (1) on the body or on a vehicle door and/or in the vehicle interior.

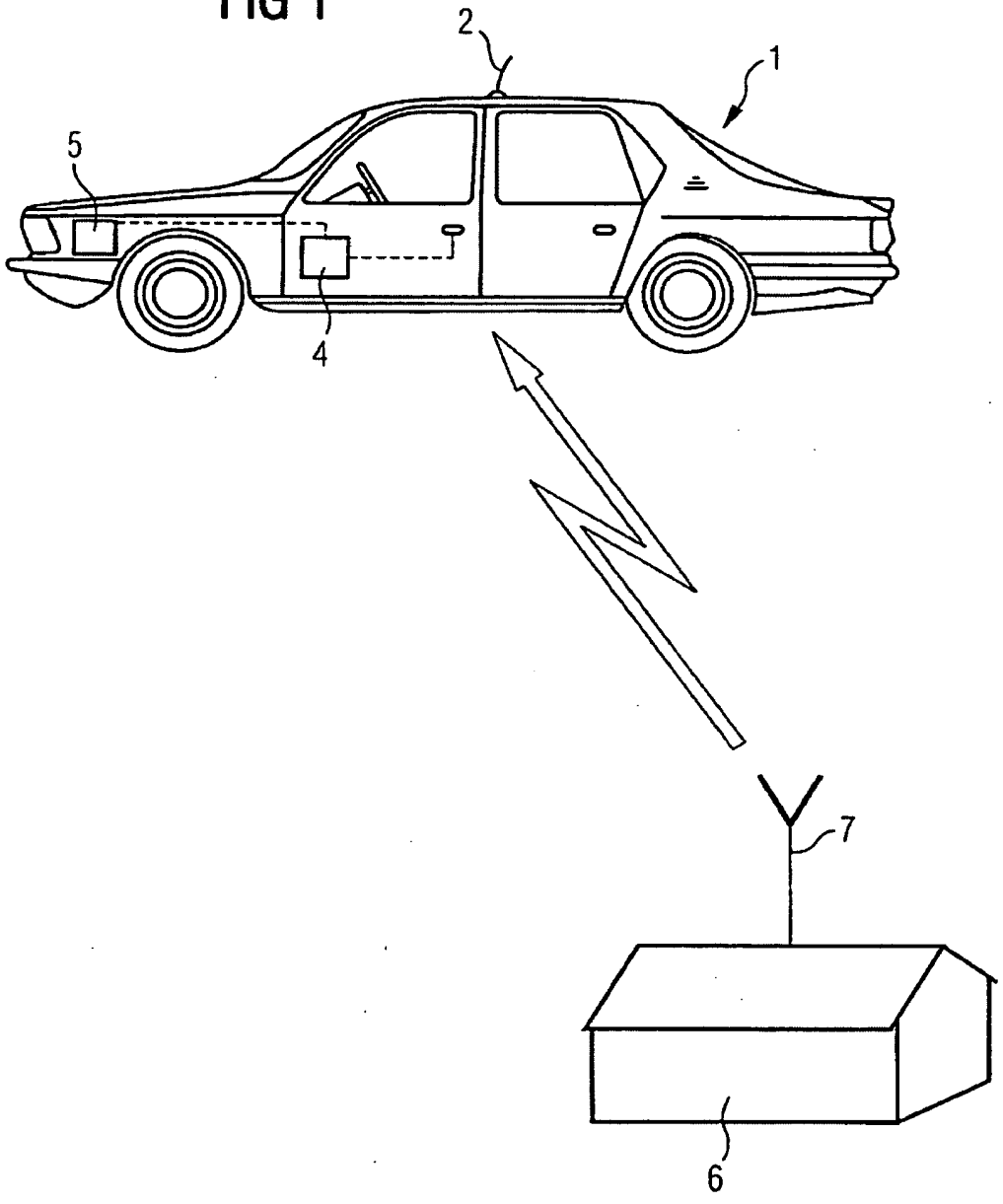
7. Security device according to claim 1, characterized in that the authorization data have person-specific biometric data.

8. Security device according to claim 1, characterized in that the authorization data have use data through which an extent of use of the vehicle is specified.

9. Security device against unauthorized use of an object, with
- a receiving device (2), that receives object- and/or person-specific initialization data via a communications system,
- a biometric identification arrangement (8, 9, 10) that detects biometric characteristics of a user and processes them into identification data when the initialization data had been received in advance, and
- a storage unit (11) in which the identification data are stored as a result of receiving the initialization data through the identification arrangement (8, 9, 10) as future comparative data.

10. Security device according to claim 9, characterized in that the object has an input means (30) by means of which encoded information is entered, which is compared with encoded reference information transmitted via the communications system along with the initialization data.

FIG 1



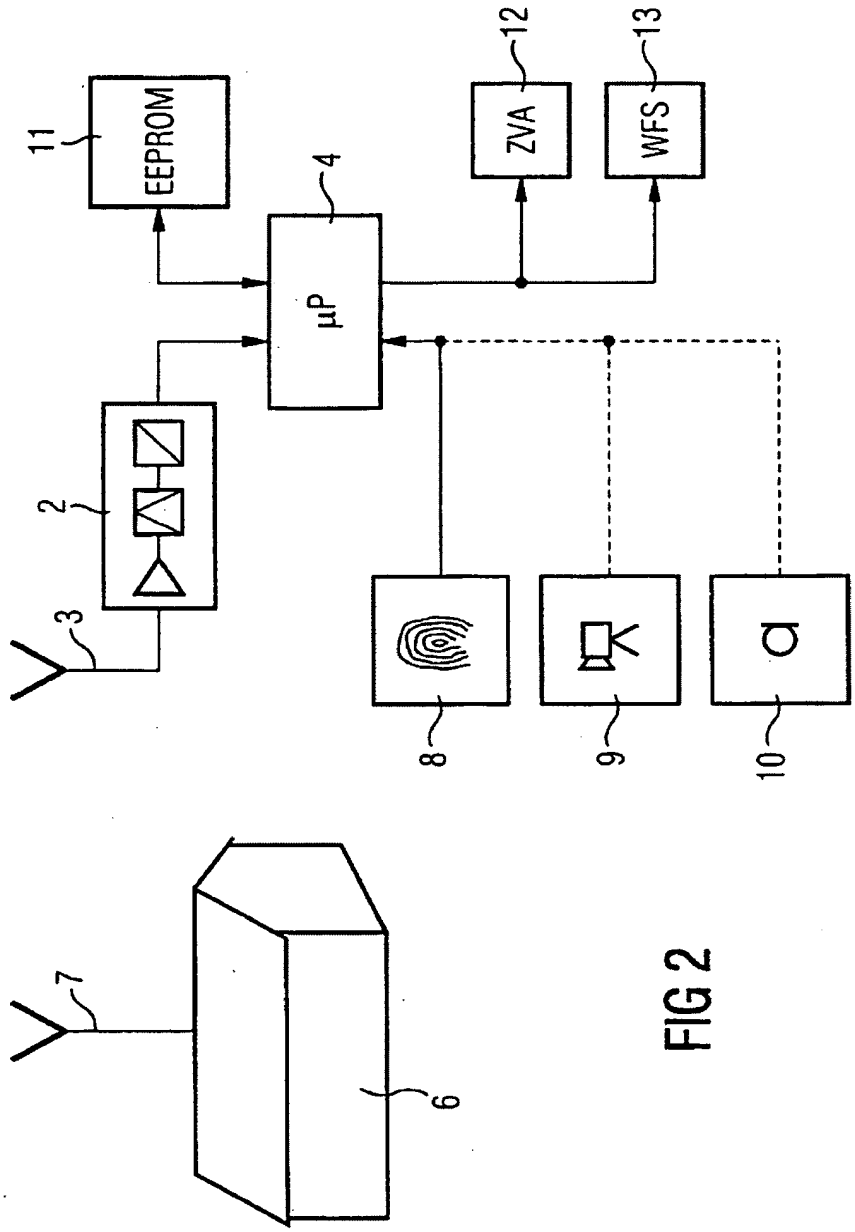


FIG 2

Key:
12 ZVA = central locking system;
13 WFS = drive-off lock

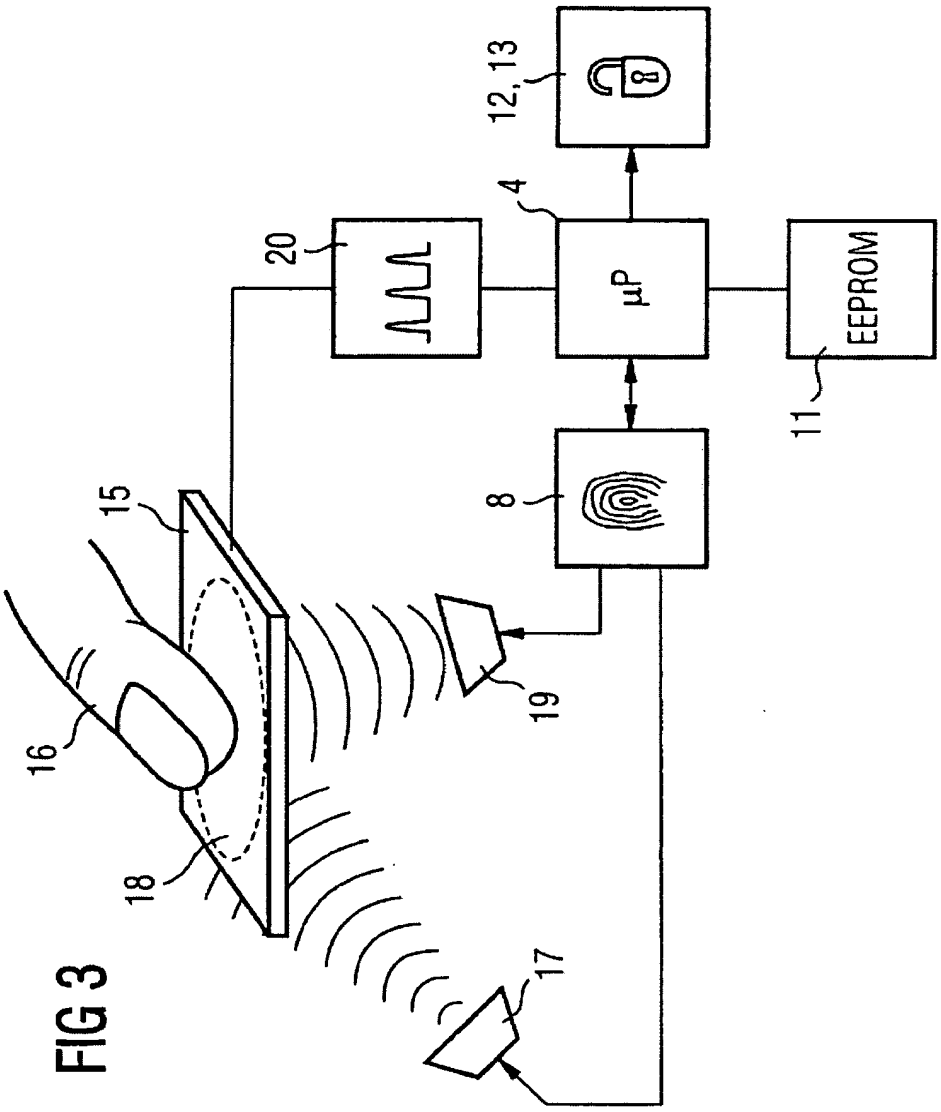
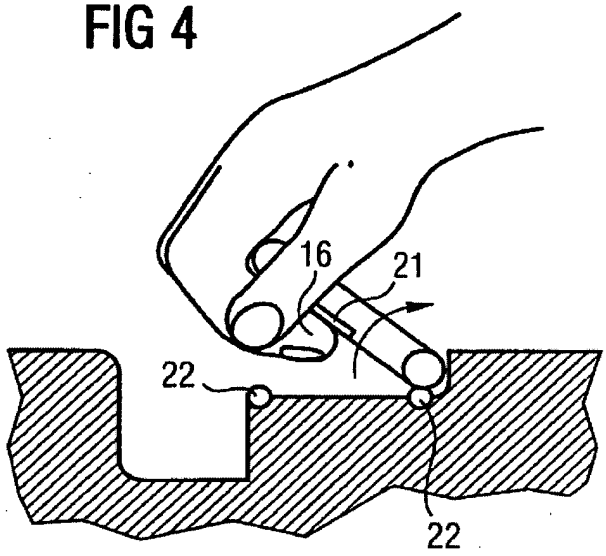


FIG 3

FIG 4



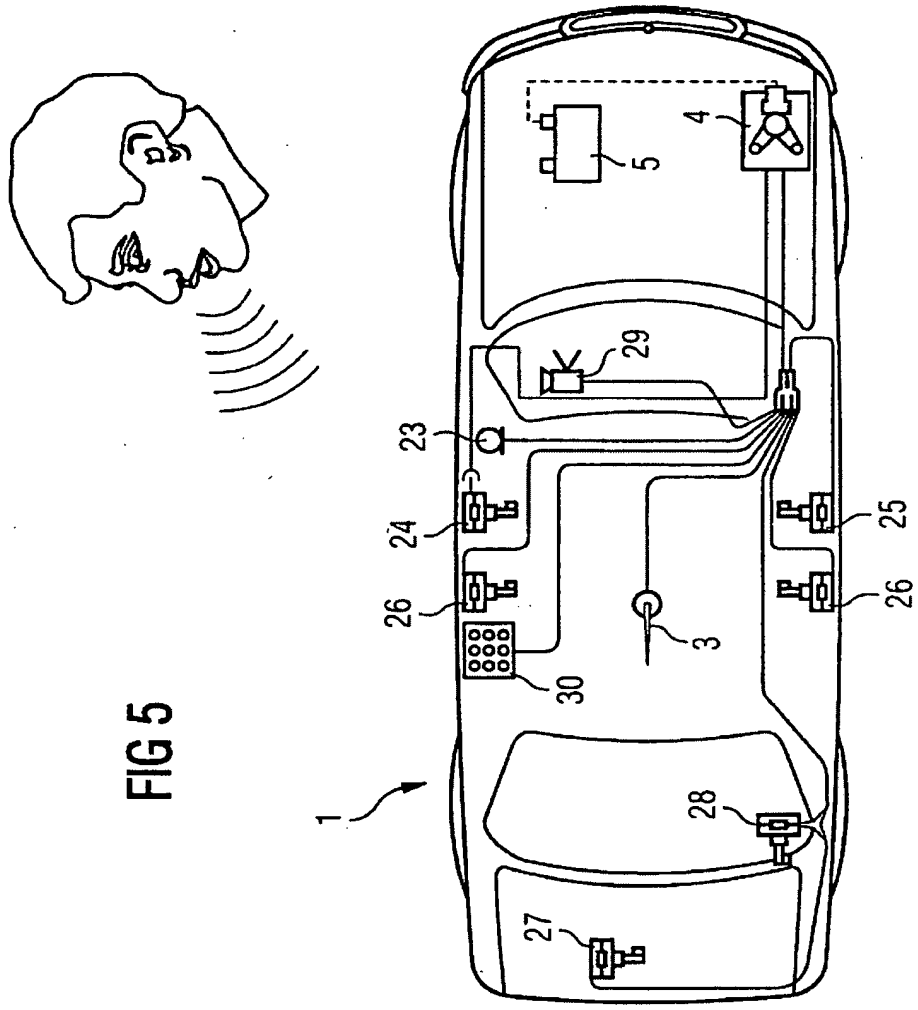


FIG 5

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :
G07C 9/00, B60R 25/00

A1

(11) Internationale Veröffentlichungsnummer: WO 99/23614

(43) Internationales Veröffentlichungsdatum: 14. Mai 1999 (14.05.99)

(21) Internationales Aktenzeichen: PCT/DE98/03182

(22) Internationales Anmeldedatum: 30. Oktober 1998 (30.10.98)

(30) Prioritätsdaten:
197 48 325.9 31. Oktober 1997 (31.10.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: LÖFFLER, Maximilian [DE/DE]; Wanderweg 8a, D–93170 Bernhardswald (DE).

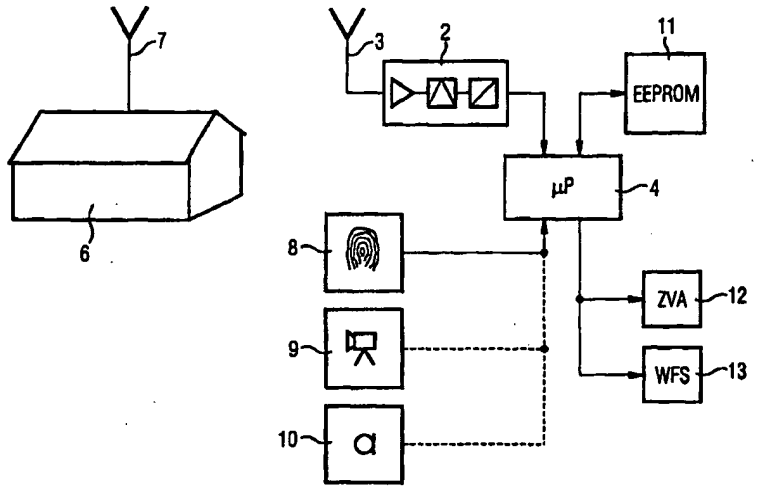
(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D–80506 München (DE).

(81) Bestimmungsstaaten: BR, CN, JP, KR, MX, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: SECURITY DEVICE AGAINST UNAUTHORIZED USE, ESPECIALLY OF A MOTOR VEHICLE

(54) Bezeichnung: SICHERHEITSEINRICHTUNG GEGEN UNBEFUGTE BENUTZUNG, INSBESONDERE EINES KRAFTFAHRZEUGS



(57) Abstract

The security device comprises a receiver (2) that picks up comparative data emitted by a central office (6) by means of a communications system. The comparative data is stored in a setpoint storage (11). In order to gain access to the object (1), biometric characteristics of the user are detected and compared with the stored comparative data. Use of the object (1) is made possible when said characteristics and the comparative data match.

(57) **Zusammenfassung**

Die Sicherheitseinrichtung weist einen Empfänger (2) auf, der Vergleichsdaten über ein Kommunikationssystem von einer Zentrale (6)empfängt. Die Vergleichsdaten werden in einem Sollwertspeicher (11) gespeichert. Für den Zugang zu dem Objekt (1) werden biometrische Merkmale eines Benutzers erfaßt und mit den gespeicherten Vergleichsdaten verglichen. Bei Übereinstimmung wird die Benutzung des Objekts (1) ermöglicht.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Beschreibung

Sicherheitseinrichtung gegen unbefugte Benutzung, insbesondere eines Kraftfahrzeugs

Die Erfindung betrifft eine Sicherheitseinrichtung gegen unbefugte Benutzung, insbesondere eines Kraftfahrzeugs, wie eines Leasing- oder Mietfahrzeugs oder eines Fahrzeugs einer Fahrzeugflotte. Mit dieser Sicherheitseinrichtung soll ein Benutzen eines Objektes, insbesondere das Benutzen eines Fahrzeugs nur bei Nachweis einer Berechtigung möglich sein.

Bei einer bekannten Sicherheitseinrichtung (DE 195 08 370 A1) findet eine bidirektionale Kommunikation zwischen einem Kraftfahrzeug und einer Zentrale statt. Dabei werden von der Zentrale Freigabesignale zu dem Kraftfahrzeug ausgesendet. Mit den Freigabesignalen wird auch eine Benutzungsbeschränkung des Fahrzeugs festgelegt. Wenn der Benutzer sein Fahrzeug mit einem Schlüssel öffnet, so wird nachgefragt, ob eine Benutzungsberechtigung vorliegt. Falls eine Berechtigung vorliegt, so kann das Fahrzeug in dem mit dem Freigabesignal mitgeteilten Umfang genutzt werden.

Wenn ein Unberechtigter in den Besitz des Schlüssels kommt, so kann er das Fahrzeug benutzen, solange das von der Zentrale ausgesendete Freigabesignal vorliegt. Wenn in der Zentrale noch nicht bekannt ist, daß der Fahrzeugschlüssel gestohlen wurde, so kann der Unberechtigte das Fahrzeug weiter nutzen.

Eine weitere bekannte Sicherheitseinrichtung (US 4,353,056 oder DE 42 22 387 C2) weist eine biometrische Identifikationsvorrichtung auf, mit der ein Fingerabdruck eines Benutzers erfaßt wird, bevor der Zugang zu dem Fahrzeug freigegeben wird. Bei solchen Sicherheitseinrichtungen kann nur der anfänglich einmal festgelegte Benutzer das Fahrzeug in einem

definierten Umfang benutzen. Falls ein Leasing- oder Mietfahrzeug den Besitzer oder Benutzer wechselt, so müssen die Berechtigungsdaten des neuen Benutzers bereits vorab im Fahrzeug hinterlegt sein, damit dieser das Fahrzeug ordnungsgemäß nutzen kann.

Aufgabe der Erfindung ist es, eine unbefugte Benutzung eines Objekts, insbesondere eines Leasing- oder Mietfahrzeugs oder eines Fahrzeugs einer Fahrzeugflotte, zuverlässig und auf einfache Weise zu verhindern.

Diese Aufgabe wird erfindungsgemäß durch die Merkmale der Patentanspruch 1 und 8 gelöst. Dabei weist die Sicherheitseinrichtung einerseits eine biometrische Identifikationsvorrichtung auf, mit der biometrische Merkmale eines Benutzers erfaßt werden. Bei Zugang zu dem Kraftfahrzeug werden diese biometrischen Merkmale mit gespeicherten Vergleichsdaten verglichen. Bei Übereinstimmung wird die Benutzung des Fahrzeugs zugelassen. Damit die Vergleichsdaten jederzeit geändert werden können, weist die Sicherheitseinrichtung andererseits eine Empfangseinrichtung auf, über die Berechtigungsdaten über ein Kommunikationssystem empfangen werden. Diese Berechtigungsdaten werden entweder als Vergleichsdaten gespeichert oder zum Einleiten einer Initialisierung und anschließendem Speichern der Vergleichsdaten verwendet.

Mit dieser Sicherheitseinrichtung kann das Leasing- oder Mietfahrzeug an einen anderen Besitzer weitergegeben werden, wobei die Berechtigungsdaten zuvor in einer Zentrale erfaßt und über das Kommunikationssystem zu dem Fahrzeug gesendet werden. In dem Fahrzeug brauchen nicht alle Berechtigungsdaten von jedem zukünftigen Benutzer im Kraftfahrzeug gespeichert sein. Benutzer eines Kraftfahrzeugs können daher beliebig wechseln, solange sie als Benutzer in der Zentrale bekannt sind. Schlüssel zum Benutzen des Kraftfahrzeugs brau-

chen nicht von einem Benutzer an den nächsten weitergegeben zu werden. Im Kraftfahrzeug können nur die Daten eines Benutzers gespeichert sein.

Bei einer Fahrzeugflotte kann somit festgelegt werden, daß ein Fahrzeug von einem ersten Fahrer und nach einer bestimmten Zeit von einem zweiten Fahrer benutzt wird. Der Umfang der Benutzung kann mit den Berechtigungsdaten jeweils vor dem Fahrerwechsel zum Fahrzeug übertragen werden.

Mit dieser Sicherheitseinrichtung kann die Initialisierung am Standort des Kraftfahrzeugs stattfinden. Allerdings wird der Beginn der Initialisierung von der Zentrale freigegeben.

Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen gekennzeichnet. So kann die biometrische Identifikationsvorrichtung eine Fingerabdruckerkennungseinheit, eine Spracherkennungseinheit oder eine Bilderkennungseinheit sein, mit der die biometrischen Merkmale eines Benutzers erfaßt werden. Ein Benutzer braucht somit keinen Schlüssel bei sich zu tragen, mit dem er das Fahrzeug aufschließen muß und das Kraftfahrzeug starten kann.

Wenn die erfaßten biometrischen Merkmale mit den Vergleichsdaten übereinstimmen, so kann sowohl eine Zentralverriegelungsanlage als auch eine Wegfahrsperre angesteuert werden. Die biometrische Identifikationsvorrichtung ist vorzugsweise derart am oder im Kraftfahrzeug angeordnet, daß mit Benutzern, die sowohl von außen kommen als auch im Fahrzeug sitzen, eine biometrische Identifikation durchgeführt werden kann. Vorzugsweise ist die Identifikationsvorrichtung am oder in der Nähe eines Schlosses (Türschloß oder Zündschloß) eines Kraftfahrzeugs angeordnet. Somit kann sowohl der Zugang zum Kraftfahrzeug als auch das Starten des Kraftfahrzeugs nur bei Berechtigung gewährleistet werden.

Die Berechtigungsdaten können personenbezogene, biometrische Daten oder auch objektspezifische Benutzungsdaten sein, mit dem der Umfang der Benutzung festgelegt wird. Als Berechtigungsdaten können auch Steuerdaten übertragen werden, aufgrund derer eine Initialisierung eingeleitet wird, nach deren erfolgreichen Verlauf Vergleichsdaten des die Initialisierung durchführenden Benutzers gespeichert werden. Die Initialisierung wird dann durchgeführt, wenn eine Pincodenummer korrekt über eine Tastatur eingegeben wird.

Ausführungsbeispiele der Erfindung werden im folgenden anhand der schematischen Zeichnungen näher erläutert. Es zeigen:

Figur 1: ein Kraftfahrzeug mit einer erfindungsgemäßen Sicherheitseinrichtung, das mit einer Zentrale über ein Kommunikationssystem kommuniziert,

Figur 2: ein Blockschaltbild der Sicherheitseinrichtung nach Figur 1,

Figur 4: ein Blockschaltbild der biometrischen Identifikationsvorrichtung,

Figur 3: eine biometrische Identifikationsvorrichtung, die an einem Türgriff angeordnet ist, und

Figur 5: ein weiteres Ausführungsbeispiel der biometrischen Identifikationsvorrichtung.

Eine erfindungsgemäße Sicherheitseinrichtung gegen unbefugtes Benutzen eines Objekts wird im folgenden am Ausführungsbeispiel der Benutzung eines Kraftfahrzeugs erläutert. Die Sicherheitseinrichtung kann auch bei vielen anderen Objekten verwendet werden, bei denen vor Benutzung des Objekts eine Berechtigung nachgewiesen werden muß.

Ein Kraftfahrzeug 1 (Figur 1) weist eine Sende- und Empfangseinrichtung 2 (vgl. auch Figur 2) auf, die mit einer Antenne

3 im oder am Kraftfahrzeug 1 verbunden ist. Die Sende- und Empfangseinrichtung 2 ist mit einer Steuereinheit 4 verbunden, in der empfangenen Daten ausgewertet und zu sendende Daten aufbereitet werden. Die Steuereinheit 4 ist weiterhin mit einer biometrischen Identifikationsvorrichtung verbunden, die biometrische Merkmale eines Benutzers erfaßt und zu Identifikationsdaten verarbeitet. Die Sende- und Empfangseinrichtung 2 und die Steuereinheit 4 werden von einer Fahrzeugbatterie 5 mit Energie versorgt.

Die Sicherheitseinrichtung im Kraftfahrzeug 1 kommuniziert mit einer Zentrale 6 über ein Kommunikationssystem. Die Zentrale 6 kann über eine Sende-/Empfangsantenne 7 Daten zu dem Kraftfahrzeug 1 senden und welche von dort empfangen.

Bei dem Kommunikationssystem kann es sich beispielsweise um ein Mobiltelefon- oder Mobilfunksystem handeln, bei dem die fahrzeugseitige Telefonanlage selbsttätig Verbindung zu der Zentrale 6 herstellen kann. Das Kommunikationssystem kann auch ein Satellitenkommunikationssystem sein, bei dem Daten von einer Zentrale 6 über geostationäre Satelliten zum Kraftfahrzeug 1 und umgekehrt gesendet werden. Das Kommunikationssystem kann auch ein sonstiges Funksystem sein, bei dem eine Datenübertragung zwischen einem Objekt und einer Zentrale 6 stattfindet. Die Ausgestaltung des Kommunikationssystems ist für die Erfindung unwesentlich. Wesentlich ist, daß Daten zwischen einer Zentrale 6 und einem Objekt übertragen werden.

Die Datenübertragung zwischen dem Kraftfahrzeug 1 und der Zentrale 6 oder umgekehrt erfolgt dabei in verschlüsselter/codierter Form, damit ein Mithören der Daten und Gebrauchen durch Unberechtigte erschwert wird. Die Daten enthalten stets eine objekt- oder fahrzeugspezifische Kennung, damit ein Verwechseln von Fahrzeugen verhindert wird.

Die fahrzeugseitige Sicherheitseinrichtung weist die Sende- und Empfangseinrichtung 2 (Figur 2) auf, die über die Antenne 3 Signale von der Zentrale 6 empfängt. Diese Signale werden in der Sende- und Empfangseinrichtung 2 demoduliert und gewandelt und der zentralen Steuereinheit 4 zugeführt. Der Steuereinheit 4 werden ebenfalls biometrische Daten zugeleitet, die bei Zugangswunsch zu dem Kraftfahrzeug 1 durch die biometrische Identifikationsvorrichtung erfaßt werden.

Als Identifikationsvorrichtung wird vorteilhafterweise eine Fingerabdruckerkennungseinheit 8 verwendet. Ebenso kann eine Bilderkennungseinheit 9 oder eine Spracherkennungseinheit 10 als Identifikationsvorrichtung dienen.

Bei Zugangswunsch wird entsprechend ein Fingerabdruck eines Benutzers mit der Fingerabdruckerkennungseinheit 8, ein Körpermerkmal oder biometrische Muster, wie beispielsweise das Gesicht des Benutzers oder die charakteristische Iris im Auge des Benutzers mit der Bilderkennungseinheit 9, oder die Sprache des Benutzers mit der Spracherkennungseinheit 10 erfaßt. Die erfaßten Daten werden gewandelt (digitalisiert) und der Steuereinheit 4 aufbereitet zugeführt. Dort werden die Daten ausgewertet.

Das Steuereinheit 4 vergleicht die Identifikationsdaten, die durch die biometrische Identifikationsvorrichtung erfaßt wurden, mit Vergleichsdaten, die in einem Sollwertspeicher 11 gespeichert sind. Die Vergleichsdaten sind diejenigen Daten, die erwartet werden, wenn sich ein Benutzer authentifiziert (Nachweis seiner Berechtigung).

Wenn zumindest ein Teil der erfaßten Identifikationsdaten mit den gespeicherten Vergleichsdaten übereinstimmen, so wird ein Steuersignal erzeugt und an ein Sicherheitsaggregat, wie eine Zentralverriegelungsanlage 12 oder eine Wegfahrsperre 13 ge-

leitet. Somit können die Türen des Fahrzeugs entriegelt oder die Wegfahrsperre 13 gelöst werden.

Die biometrische Identifikationsvorrichtung ist für Kraftfahrzeuge vorzugsweise als Fingerabdruckerkennungseinheit 8 ausgebildet. Diese weist einen Sensor 15 (Figur 3) zum Erfassen des Fingerabdrucks auf, der von außerhalb des Kraftfahrzeugs 1 für den Benutzer gut zugänglich an der Karosserie angeordnet ist. Zum Erfassen des Fingerabdrucks legt der Benutzer einen oder mehrere Finger 16 auf den Sensor 15. Dabei kann je nach Erfassungsmethode der "äußere" Fingerabdruck (Rillen- und Furchenmuster) oder auch der "innere" Fingerabdruck (Struktur der Epidermis) erfaßt werden.

Über ein Sendeelement 17 wird ein Signal, z.B. optisch oder akustisch, zu dem Sensor 15 mit seiner Sensorfläche/Auflagefläche 18 ausgesendet. Von der Sensorfläche 18 gehen die Signale zum Teil in den Finger 16 oder werden von dessen Oberfläche zur Sensorfläche 18 reflektiert. Die von dem Sensor 15 infolge Reflexion zurückkommenden Signale werden über ein Empfangselement 19 empfangen und der Fingerabdruckerkennungseinheit 8 zugeleitet. Der digitalisierte und ausgewertete Muster des Fingerabdrucks wird dem Steuereinheit 4 zugeführt und - ähnlich wie in DE 42 22 387 C2 beschrieben - dort weiterbehandelt.

Das Erfassen des Fingerabdrucks kann auch mit kapazitiven Elektroden - wie in der Patentschrift US 4,353,056 beschrieben - von statten gehen. Es gibt noch viele andere Möglichkeiten, den Fingerabdruck zu erfassen und auszuwerten. Da Fingerabdruckerkennungseinheiten und deren Funktionsweise hinreichend bekannt sind, wird hierauf nicht mehr näher eingegangen.

Um sicher zu gehen, daß der Fingerabdruck von einer lebenden Person stammt, kann zusätzlich eine Vitalitätserkennungseinheit 20 vorhanden sein. In dem Ausführungsbeispiel nach Figur 3 ist eine Pulserkennungseinheit als Vitalitätserkennungseinheit 20 vorgesehen, die den Puls des Fingers 16 erfaßt. Nur wenn ein Puls erkannt wird, werden die erfaßte Fingerabdrucksmuster mit erwarteten Daten, die in dem Sollwertspeicher 11 gespeichert sind, verglichen. Bei zumindest weitgehender Übereinstimmung wird die Zentralverriegelungsanlage 12 oder die Wegfahrsperre 13 gesteuert.

Es gibt noch viele weitere, bekannte Möglichkeiten, die Vitalität des Benutzers festzustellen. So können Impedanzmessungen der Haut, pulsoximetrische oder elektrokardiographische Meßverfahren, oder sonstige, gleichwertige Verfahren durchgeführt werden, auf die hier jedoch nicht näher eingegangen werden soll.

Der Sensor 15 zum Erfassen des Fingerabdrucks kann auch an einem Türgriff 21 (Figur 4) befestigt sein. Der Sensor 15 ist vorteilhafterweise auf der Innenseite des Türgriffs 21 geschützt angeordnet. Wenn ein Benutzer den Türgriff 21 zieht, so liegt zumindest ein Finger 16 auf dem Sensor 15 auf.

Damit der Sensor 15 nicht zu sehr verschmutzt wird, kann eine Dichtung 22 vorgesehen sein, an der der Türgriff 21 im nicht benutzten Zustand dicht anliegt.

Zum Erfassen der biometrischen Identifikationsdaten kann auch statt der Fingerabdruckerkennungseinheit 8 die Spracherkennungseinheit 10 verwendet werden. Hierbei ist ein Mikrophon 23 (Figur 5) in dem Kraftfahrzeug 1 derart angeordnet, daß es die von einem Benutzer gesprochenen Worte erfassen kann. Die Worte oder Sprachmuster werden dann in der Spracherkennungs-

einheit 10 gewandelt und ausgewertet sowie in der Steuereinheit 4 weiterverarbeitet.

Die Steuereinheit 4 vergleicht die erhaltenen Sprachsignale mit Sollsignalen, die in dem Sollwertspeicher 11 gespeichert sind. Falls der Benutzer anhand der gesprochenen Worte als berechtigt erkannt wird, so werden die Türschlösser des Kraftfahrzeugs 1 über die Steuereinheit 4 entriegelt.

Die Zentralverriegelungsanlage 12 umfaßt ein Fahrertürschloß 24, ein Beifahrertürschloß 25, zwei Fontschlösser 26, ein Heckdeckelschloß 27 und - falls vorhanden - ein Tankdeckelschloß 28. Diese Schlösser können durch die Steuereinheit 4 - zum Teil einzeln oder alle zusammen - ver- oder entriegelt werden, wenn der Benutzer als berechtigt erkannt wird.

Wenn das Kraftfahrzeug 1 entriegelt ist, so kann der Benutzer in das Kraftfahrzeug 1 einsteigen und den Motor starten. Auch zum Starten des Motors kann eine biometrische Authentifikation (Fingerabdruckerkennung, Spracherkennung oder Bilderkennung) Voraussetzung sein. Daher sind dann im Inneren des Kraftfahrzeugs 1 ein weiterer Sensor zum Erfassen des Fingerabdrucks, ein weiteres Mikrophon zum Erfassen der Sprache oder eine Videokamera 29 zur Bilderkennung angeordnet. Beim Startversuch wird die biometrischen Identifikationsvorrichtung aktiviert. Bei erfolgreicher Authentifikation (Berechtigung ist nachgewiesen) kann das Fahrzeug ordnungsgemäß benutzt werden, da erst dann die Wegfahrsperre 13 gelöst wird.

Herkömmlicherweise sind in dem Sollwertspeicher 11 erwartete biometrische Daten eines Benutzers gespeichert. Diese Daten wurden bei einer Initialisierung der Sicherheitseinrichtung erfaßt. Bei der Initialisierung wird erstmalig ein Benutzer zum Benutzen eines Kraftfahrzeugs 1 zugelassen, indem seine Berechtigungsdaten gespeichert werden.

Mit der erfindungsgemäßen Sicherheitseinrichtung können die biometrischen Daten in einer Zentrale 6 einmalig oder mehrmals erfaßt werden. Dort kann jeder Benutzer, der das Fahrzeug benutzen darf, seine biometrischen Merkmale in Form der Identifikationsdaten erfassen lassen. Die biometrischen Daten können in der Zentrale 6 für Dritte unzugänglich gespeichert bleiben.

Über die Zentrale 6 werden dann - je nach Bedarf - die entsprechenden Berechtigungsdaten zu dem Kraftfahrzeug 1 gesendet, d.h. die biometrischen Daten desjenigen Benutzers, der das Fahrzeug benutzen darf, werden als Berechtigungsdaten zum Fahrzeug gesendet. Dort werden die Berechtigungsdaten in den Sollwertspeicher 11 gespeichert. Dabei können die bisherigen Berechtigungsdaten überschrieben oder gelöscht werden. Es können auch Berechtigungsdaten von mehreren Benutzern gleichzeitig dort gespeichert sein. Dann dürfen mehrere Benutzer das Kraftfahrzeug 1 benutzen.

Ein neuer Benutzer kann auch nachträglich für das Fahrzeug zugelassen werden, indem er in der Zentrale 6 seine Berechtigungsdaten durch eine biometrische Identifikationsvorrichtung erfassen läßt. Die erfaßten Identifikationsdaten werden dann als Berechtigungsdaten zu dem Fahrzeug übertragen und in dem Sollwertspeicher 11 gespeichert.

Zusammen mit den Berechtigungsdaten können auch Nutzungsdaten übertragen werden, durch die der Umfang der Benutzung des Kraftfahrzeugs 1 festgelegt wird. Der Umfang der Benutzung kann dabei eine Zeitdauer, ein geographisches Benutzungsgebiet, eine maximale Fahrstrecke, eine Anzahl von Benutzern oder eine codierte Information sein. Die Nutzungsdaten werden als digitaler Wert zusammen mit den Berechtigungsdaten ver-

schlüsselt oder codiert zum Kraftfahrzeug 1 moduliert übertragen.

Sobald die Berechtigungsdaten empfangen sind, werden sie demoduliert und entschlüsselt sowie in dem Sollwertspeicher 11 gespeichert. Das Kraftfahrzeug 1 ist dann für den jeweiligen berechtigten Benutzer in dem durch die Nutzungsdaten festgelegten Umfang betriebsbereit.

Der berechtigte Umfang der Benutzung kann durch bekannte Einrichtungen, wie einer Uhr, einem Kilometerzähler, einem GPS-Ortungssystem u.ä. überwacht werden. Bei Überschreiten des Umfangs kann der Benutzer und die Zentrale 6 gewarnt werden. Bei weiterer Überschreitung kann das Kraftfahrzeug 1 von der Zentrale 6 aus angehalten und verriegelt werden, d.h. die Benutzungserlaubnis wird widerrufen.

Als Berechtigungsdaten können auch ein Initialisierungssteuersignal zusammen mit einer codierten Sollinformation, z.B. eine Pincodenummer, zum Kraftfahrzeug 1 übertragen werden. Wird die dem Benutzer bereits vorab bekanntgemachte Pincodenummer am Fahrzeug über eine Tastatur 30 korrekt eingegeben, so werden die Türen entriegelt und eine Lernprozedur (als Initialisierung bezeichnet) für personenbezogene, biometrische Daten gestartet. Bei der Initialisierung werden die Identifikationsdaten einmal erfaßt als Berechtigungsdaten abgespeichert. Eine neue Initialisierung kann erst wieder durchgeführt werden, wenn wieder ein Initialisierungssteuersignal von der Zentrale 6 empfangen wird.

Statt einer Pincodenummer kann auch eine sonstige codierte Information zum Kraftfahrzeug übertragen werden. Dann wird - anstatt der Tastatur 30 - ein anderes Eingabemittel benötigt, mit dem eine codierte Information vom Benutzer eingegeben wird. Ein solches Eingabemittel kann beispielsweise ein vom

Vermieter oder Flottenbetreiber zur Verfügung gestellter Handsender oder eine Chipkarte sein. Diese liefern ihre codierte Information an das Kraftfahrzeug, wo sie mit der empfangenen Sollinformation verglichen wird. Bei Übereinstimmung wird die Lernprozedur wie - oben beschrieben - gestartet.

Hierzu wird beispielsweise die Fingerabdruckerkennungseinheit 8 aktiviert, auf deren Sensor 15 der jeweilige Benutzer seinen Finger 16 legt. Der erfaßte Fingerabdruck wird verarbeitet und zu Vergleichsdaten umgewandelt. Die Vergleichsdaten werden dann in den Sollwertspeicher 11 gespeichert. Nach Beendigung der Initialisierung kann dieser Benutzer das Fahrzeug im Rahmen der festgelegten Benutzung benutzen.

Dies hat den Vorteil, daß der Benutzer nicht vorher in der Zentrale 6 gewesen sein muß, um seine Berechtigungsdaten zu hinterlegen. Allerdings kann er die Initialisierung nur dann durchführen, wenn einerseits das Initialisierungssteuersignal empfangen wurde und andererseits eine zusätzliche Berechtigung nachgewiesen wird. Die zusätzliche Berechtigung kann durch Eingeben der codierten Information nachgewiesen, falls die eingegebene Information mit der zuvor empfangenen Sollinformation übereinstimmt.

Für den Vorgang der Initialisierung können zeitliche Grenzen gesetzt werden, innerhalb derer die Initialisierung durchgeführt werden muß. Falls die Initialisierung nicht innerhalb der gesetzten Frist durchgeführt ist, so können alle bisherigen Vergleichsdaten weiterhin Geltung haben oder sie können gelöscht werden, so daß niemand berechtigt ist, das Kraftfahrzeug 1 zu benutzen, außer neue Berechtigungsdaten werden wieder von der Zentrale 6 übertragen oder eine erneute Initialisierung wird durchgeführt.

Die übermittelte Pincodenummer darf sicherheitshalber nur dem Fahrzeugverleiher und dem Fahrzeugmieter, sprich dem Benutzer, bekannt sein, um einem Mißbrauch vorzubeugen.

Es kann auch vorgesehen sein, daß die gespeicherten Vergleichsdaten nur eine vorgegebene Zeit lang gültig sind. Danach erlischt ihre Gültigkeit. Dies kann dadurch geschehen, daß der Speicherinhalt des Sollwertspeichers 11 mit den Vergleichsdaten gelöscht wird. Dem Sollwertspeicher 11 müssen dann neue Vergleichsdaten zugeführt werden, bevor das Fahrzeug wieder ordnungsgemäß benutzt werden kann.

Die biometrische Identifikationsvorrichtung kann im wesentlichen in dem Steuereinheit 4 angeordnet sein, aus der die Verbindungen zu dem Sensor 15, dem Mikrophon 23 oder der Videokamera 29 herausgeführt sind. Das Steuereinheit 4 kann dabei in einem aufbruchssicheren Gehäuse untergebracht sein.

Lediglich der Sensor 15, das Mikrophon 23 oder die Videokamera 29 zum Erfassen der biometrischen Merkmale müssen an entsprechender Stelle außerhalb der Steuereinheit angeordnet sein, damit die biometrischen Merkmale eines Benutzers einfach erfaßt werden können.

So kann der Sensor 15 der Fingerabdruckerkennungseinheit 8 an der Fahrzeugtür und ein weiterer Sensor in der Nähe des Zündschlosses 31, am Armaturenbrett in Griffweite des Benutzers, auf der Mittelkonsole oder am Schalthebel angeordnet sein. Die Videokamera 29 kann derart hinter einer Scheibe des Fahrzeugs angeordnet sein, daß sie sowohl den Außenraum als auch den Innenraum des Fahrzeugs erfaßt. Das Mikrophon 23 ist ebenfalls derart angeordnet, daß es sowohl Sprachsignale von außen als auch von innen erfassen kann. Es können auch mehrere Mikrophone oder mehrere Videokameras vorhanden sein.

Für die Erfindung ist es unwesentlich, welche biometrischen Merkmale erfaßt werden. Wesentlich ist, daß die erfaßten biometrischen Merkmale mit den Vergleichsdaten verglichen werden. Die Vergleichsdaten werden dabei entweder über die Zentrale 6 zu dem Kraftfahrzeug 1 gesendet und dort im Sollwertspeicher 11 gespeichert oder infolge eines empfangenen Initialisierungssignals nach erfolgter Initialisierung in dem Sollwertspeicher 11 gespeichert.

Der Sollwertspeicher 11 kann ein EEPROM oder ein sonstiger geeigneter Datenspeicher sein, dessen Daten von außen durch Unberechtigte nicht ausgelesen werden können. Das Steuereinheit 4 kann im wesentlichen ein Mikroprozessor oder eine funktionell gleichwertige Einrichtung sein, die die Sicherheitseinrichtung steuert. Die Berechtigungsdaten werden als digitale Signale zwischen der Zentrale 6 und dem Kraftfahrzeug 1 drahtlos auf geeignete Weise, beispielsweise als HF-Signale, ausgetauscht.

Das Steuereinheit 4 kann mit der Zentralverriegelungsanlage 12, der Wegfahrsperre 13 oder einem sonstigen Sicherheitsaggregat verbunden sein, das nur dann ver- oder entriegelt wird, wenn der Vergleich der erfaßten biometrischen Identifikationsdaten mit den Vergleichsdaten erfolgreich war.

Bei anderen Objekten, wie zum Beispiel einer Hotelanlage, kann das Kommunikationssystem ein hausinternes Datennetz mit vielen Datenleitungen sein. Über die Zentrale 6 werden die Berechtigungsdaten zu den einzelnen Sicherheitseinrichtungen (im Falle von Hotels sind dies die Türschlösser) gesendet. Somit kann die Zugangsberechtigung zu den Zimmern zentral gesteuert werden. Der Hotelgast braucht nur an der Rezeption seinen Fingerabdruck zu hinterlassen. Nach Abreise des Gastes können die Berechtigungsdaten für das Zimmer zentral gelöscht oder mit neuen Berechtigungsdaten eines anderen Hotelgastes

überschrieben werden. Im übrigen kann durch die Nutzungsdaten eine begrenzte Zeitdauer der Benutzung vorgesehen sein. Danach verfallen die Berechtigungsdaten automatisch.

Unter dem Begriff der Benutzung ist sowohl der Zugang zu einem Objekt als auch die Nutzung des Objekts selber zu verstehen. Bei einem Kraftfahrzeug 1 fällt unter die Benutzung sowohl das Entriegeln der Türschlösser als auch das Lösen der Wegfahrsperre 13.

Als Objekte können Kraftfahrzeuge, Hotelzimmer, Garagentore, mit einer Zentrale 6 vernetzte Personalcomputer oder Telefone u.ä. angesehen werden. Die erfindungsgemäße Sicherheitseinrichtung wird insbesondere für Leasing- oder Mietfahrzeug eingesetzt. Ebenso können Frachtunternehmen ihre Fahrzeugflotte (mehrere Lastkraftwagen) mit der Sicherheitseinrichtung besser vor unberechtigter Benutzung schützen. Die Fahrer können durch die Nutzungsdauer infolge der Nutzungsdaten zum Einhalten von Ruhezeiten gezwungen werden. Die Zentrale 6 kann auch ein Alarmsignal bei Überschreitung des Nutzungsumfangs empfangen und sich dann mit dem Benutzer - beispielsweise telefonisch - in Verbindung setzen.

Unter einer Wegfahrsperre 13 ist eine elektronische Einrichtung zu verstehen, die ein Starten des Verbrennungsmotors und ein Fahren nur bei Nachweis der Berechtigung ermöglicht. Die Einrichtung kann beispielsweise im Motorsteuergerät angeordnet sein. Sie gibt bei Nachweis der Berechtigung die Funktionen des Motorsteuergeräts frei. Die Einrichtung kann auch ein Ventil in der Kraftstoffleitung elektromagnetisch steuern. Ebenso ist ein gesteuerter Schalter in der Zündanlage möglich, der nur bei Nachweis der Berechtigung die Zündung des Verbrennungsmotors zuläßt. Es können auch mehrere, über das Kraftfahrzeug verteilte elektronische Einrichtungen als Wegfahrsperre dienen.

Patentansprüche

1. Sicherheitseinrichtung gegen unbefugte Benutzung, insbesondere eines Kraftfahrzeugs (1), mit
- einer biometrischen Identifikationsvorrichtung (8, 9, 10), die biometrische Merkmale eines Benutzers erfaßt und zu Identifikationsdaten verarbeitet,
- einer Empfangseinrichtung (2), die Berechtigungsdaten über ein Kommunikationssystem empfängt,
- einer Speichereinrichtung (11), in der die empfangen Berechtigungsdaten als Vergleichsdaten gespeichert werden, und
- einer Steuereinheit (3), die zumindest einen Teil der Identifikationsdaten mit den gespeicherten Vergleichsdaten vergleicht und abhängig vom Vergleichsergebnis ein Sicherheitsaggregat (12, 13) steuert.

2. Sicherheitseinrichtung nach Anspruch 1, dadurch gekennzeichnet, daß Identifikationsvorrichtung eine Fingerabdrukkerkennungseinheit (8) ist.

3. Sicherheitseinrichtung nach ein Anspruch 1, dadurch gekennzeichnet, daß die Identifikationsvorrichtung eine Spracherkennungseinheit (10) ist.

4. Sicherheitseinrichtung nach Anspruch 1, dadurch gekennzeichnet, daß die Identifikationsvorrichtung eine Bilderkennungseinheit (9) ist.

5. Sicherheitseinrichtung nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das Sicherheitsaggregat durch eine Zentralverriegelungsanlage (12) und/oder eine Wegfahrsperre (13) realisiert ist.

6. Sicherheitseinrichtung nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß zumindest ein Teil der Identifikationsvorrichtung (8, 9, 10) von außerhalb des

Kraftfahrzeugs (1) zugänglich an der Karosserie oder an einer Fahrzeugtür und/oder im Fahrzeuginneren angeordnet ist.

7. Sicherheitseinrichtung nach Anspruch 1 dadurch gekennzeichnet, daß die Berechtigungsdaten personenbezogene, biometrische Daten aufweisen.

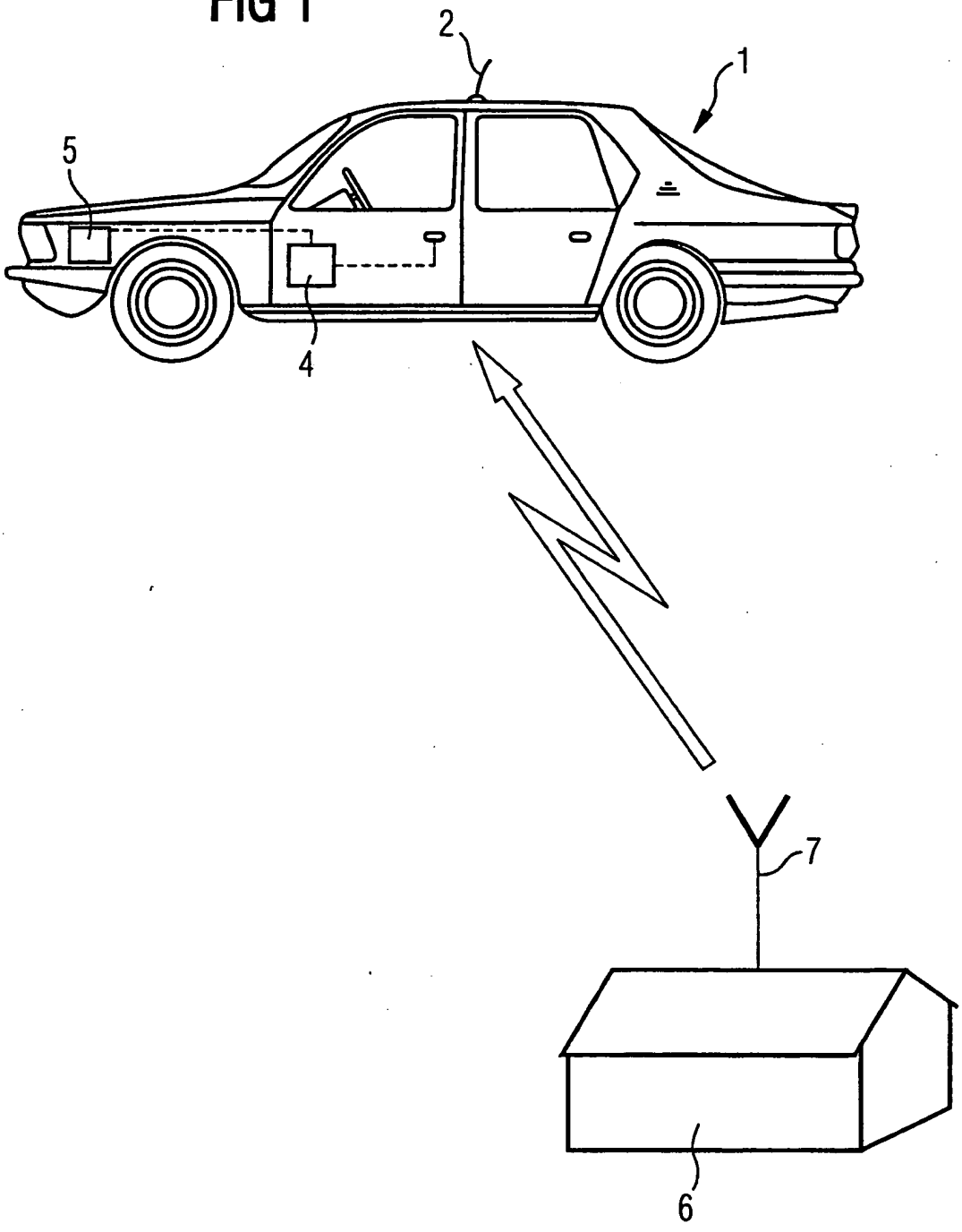
8. Sicherheitseinrichtung nach Anspruch 1 dadurch gekennzeichnet, daß die Berechtigungsdaten Nutzungsdaten aufweisen, durch die ein Umfang der Benutzung des Kraftfahrzeugs festgelegt wird.

9. Sicherheitseinrichtung gegen unbefugte Benutzung eines Objekts mit

- einer Empfangseinrichtung (2), die objekt- und/oder personenbezogene Initialisierungsdaten über ein Kommunikationssystem empfängt,
- einer biometrischen Identifikationsvorrichtung (8, 9, 10), die biometrische Merkmale eines Benutzers dann erfaßt und zu Identifikationsdaten verarbeitet, wenn zuvor die Initialisierungsdaten empfangen wurden, und
- einer Speichereinrichtung (11), in der die Identifikationsdaten infolge des Empfangs der Initialisierungsdaten durch die Identifikationsvorrichtung (8, 9, 10) als zukünftige Vergleichsdaten gespeichert werden.

10. Sicherheitseinrichtung nach Anspruch 9, dadurch gekennzeichnet, daß das Objekt ein Eingabemittel (30) aufweist, über das eine codierte Information eingeben wird, die mit einer zusammen mit den Initialisierungsdaten über das Kommunikationssystem übertragenen codierten Sollinformation verglichen wird.

FIG 1



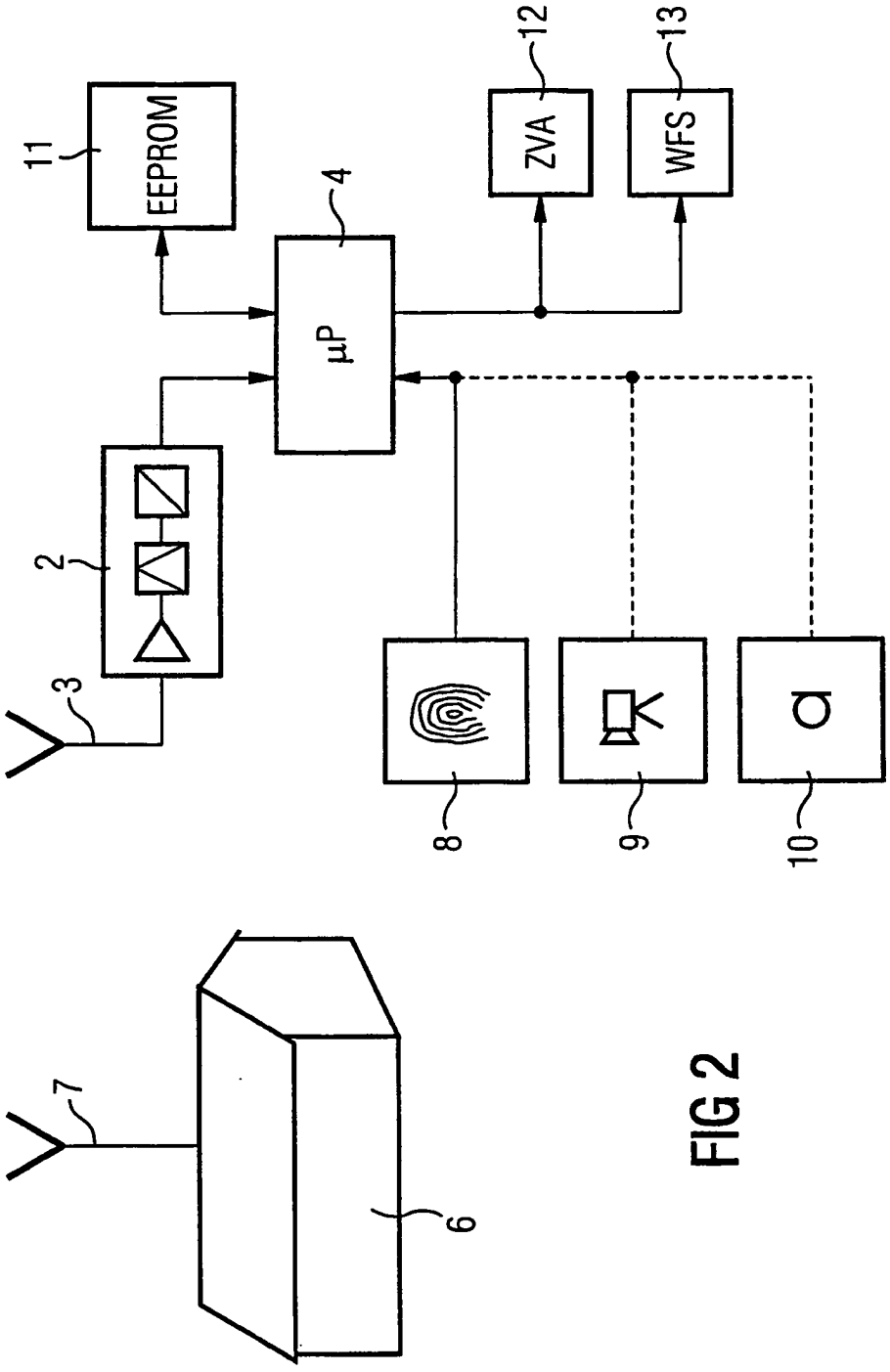


FIG 2

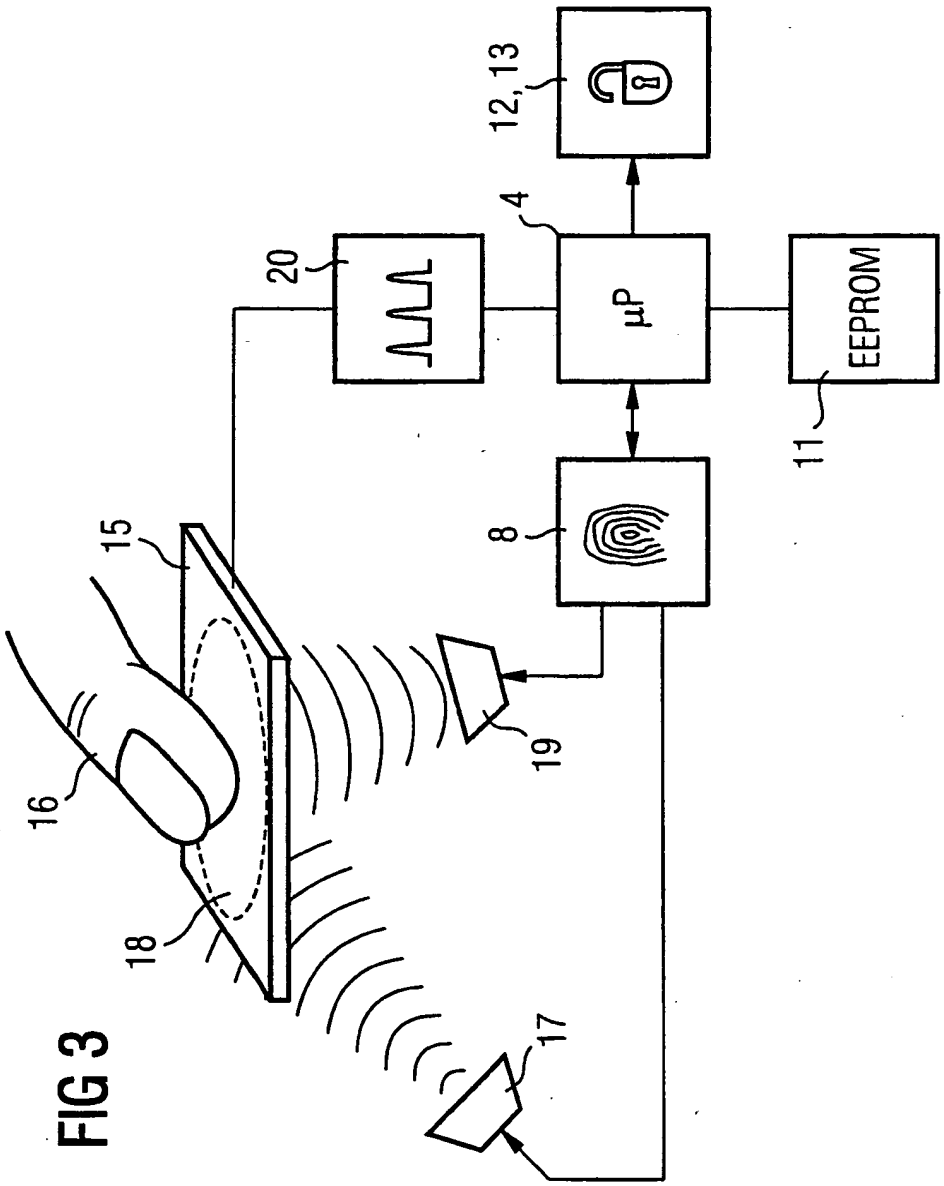
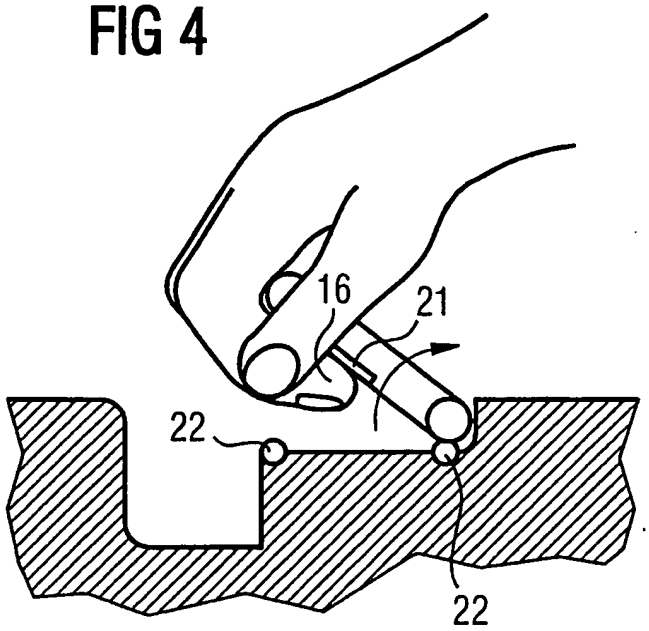


FIG 3

FIG 4



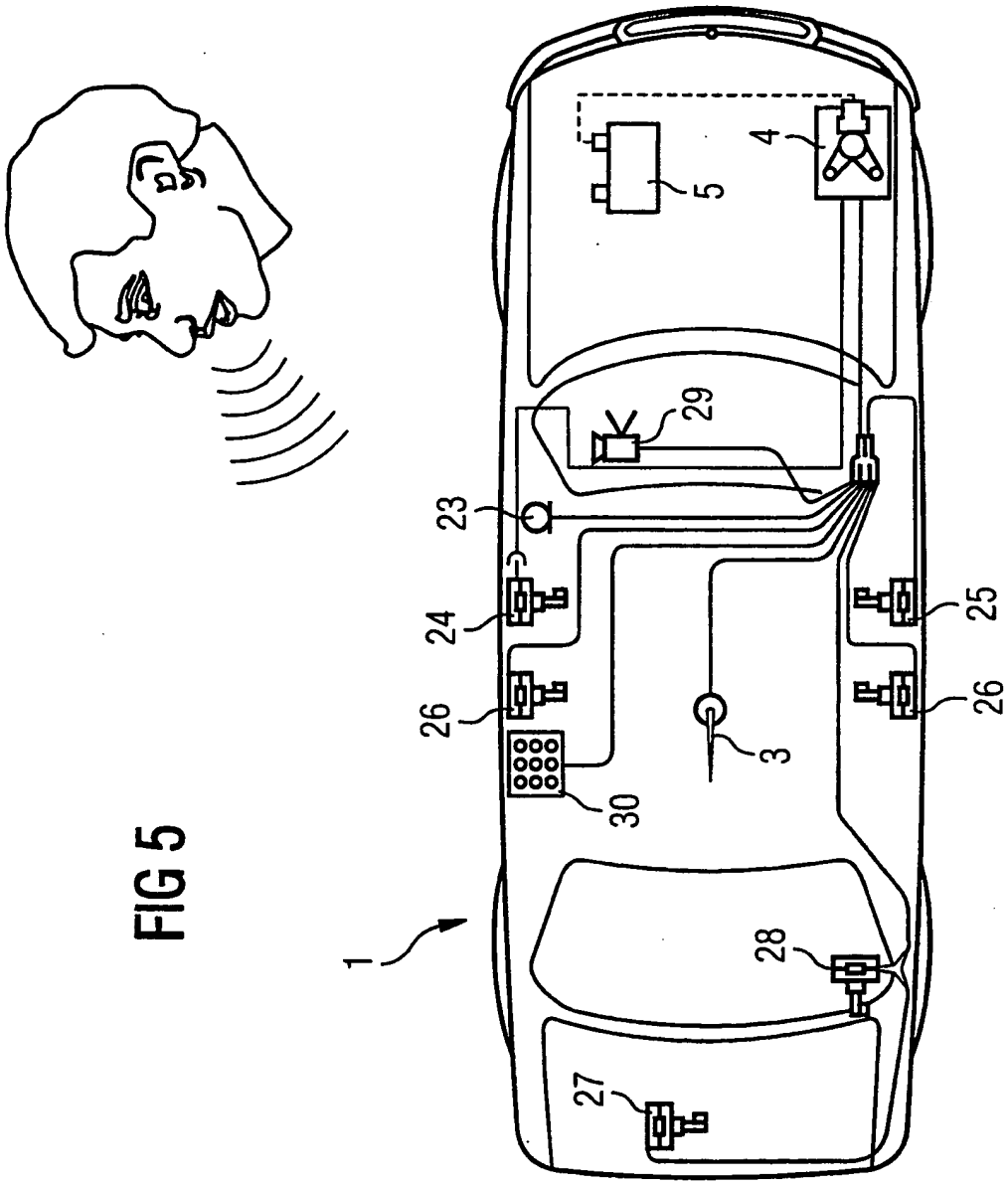


FIG 5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 98/03182

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07C9/00 B60R25/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 E05B G07C B60R G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 17237 A (PRODUCTS RESEARCH INC) 15 May 1997 see abstract; figures see page 3, line 2 - line 22 see page 11, line 14 - page 13, line 2	1,2,4-7
A	---	3,9,10
Y	DE 43 24 762 A (LATSCH UWE DIPL ING) 2 February 1995 see abstract; figure 1 see column 2, line 67 - column 4, line 21	1,3,5,8
A	---	9
Y	WO 90 00296 A (MOTOROLA INC) 11 January 1990 see abstract; figures see page 4, line 10 - page 6, line 18	1,3,5,8
	--- -/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 April 1999	14/04/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 98/03182

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	DE 43 01 039 A (LATSCH UWE DIPL ING) 21 July 1994 see abstract; figure 1 see column 1, line 54 - column 3, line 17	1,3,5, 8-10
A	US 5 055 658 A (COCKBURN JOHN B) 8 October 1991 see abstract; figures see column 1, line 52 - column 4, line 66	9
A	DE 195 08 370 A (DAIMLER BENZ AG) 12 September 1996 cited in the application	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/DE 98/03182

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9717237 A	15-05-1997	US 5660246 A	26-08-1997
		AU 1118397 A	29-05-1997
		US 5715905 A	10-02-1998
DE 4324762 A	02-02-1995	NONE	
WO 9000296 A	11-01-1990	US 5040212 A	13-08-1991
DE 4301039 A	21-07-1994	NONE	
US 5055658 A	08-10-1991	NONE	
DE 19508370 A	12-09-1996	EP 0731007 A	11-09-1996
		JP 8258670 A	08-10-1996

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 98/03182

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G07C9/00 B60R25/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 E05B G07C B60R G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 97 17237 A (PRODUCTS RESEARCH INC) 15. Mai 1997 siehe Zusammenfassung; Abbildungen siehe Seite 3, Zeile 2 - Zeile 22 siehe Seite 11, Zeile 14 - Seite 13, Zeile 2	1,2,4-7
A	---	3,9,10
Y	DE 43 24 762 A (LATSCH UWE DIPL ING) 2. Februar 1995 siehe Zusammenfassung; Abbildung 1 siehe Spalte 2, Zeile 67 - Spalte 4, Zeile 21	1,3,5,8
A	---	9
	-/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
6. April 1999	14/04/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 98/03182

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	WO 90 00296 A (MOTOROLA INC) 11. Januar 1990 siehe Zusammenfassung; Abbildungen siehe Seite 4, Zeile 10 - Seite 6, Zeile 18	1,3,5,8
A	DE 43 01 039 A (LATSCH UWE DIPL ING) 21. Juli 1994 siehe Zusammenfassung; Abbildung 1 siehe Spalte 1, Zeile 54 - Spalte 3, Zeile 17	1,3,5, 8-10
A	US 5 055 658 A (COCKBURN JOHN B) 8. Oktober 1991 siehe Zusammenfassung; Abbildungen siehe Spalte 1, Zeile 52 - Spalte 4, Zeile 66	9
A	DE 195 08 370 A (DAIMLER BENZ AG) 12. September 1996 in der Anmeldung erwähnt	

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE 98/03182

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9717237	A	15-05-1997	US	5660246 A	26-08-1997
			AU	1118397 A	29-05-1997
			US	5715905 A	10-02-1998
DE 4324762	A	02-02-1995	KEINE		
WO 9000296	A	11-01-1990	US	5040212 A	13-08-1991
DE 4301039	A	21-07-1994	KEINE		
US 5055658	A	08-10-1991	KEINE		
DE 19508370	A	12-09-1996	EP	0731007 A	11-09-1996
			JP	8258670 A	08-10-1996